

CLAIMS

Sub B

1. A user authentication system comprising a registration station provided with an information acquisition device for obtaining biological individuality data for distinguishing individuality of a user, an authentication card issuing station that issues to the user a user authentication card recorded with a divided part of the biological individuality data, an authentication access terminal provided with an authentication-card reader for reading the information of the user authentication card and an identity acquisition device for inputting biological individuality data of the user, and at least one certification authority that is connected to the authentication access terminal through an information communication channel, wherein the certification authority holds the record of the remaining part of the biological individuality data that have obtained at the registration station but not recorded in the user authentication card, the recorded contents in the user authentication card read out by the authentication card reader are compared with the biological individuality data of the user obtained on the spot through the identity acquisition device to authenticate identification of the user at the authentication access terminal, and if a higher level of authentication is required, the certification authority compares the biological individuality data of the user obtained at the authentication access terminal with the part of the biological individuality data missing in the user authentication card in response to inquiry from the authentication access terminal and sends the comparison result to the authentication access terminal

for further authentication.

2. A user authentication system according to claim 1,  
wherein the user authentication card has an computing function  
5 and the computing function executes calculation of authenticating  
personal identification at the authentication access terminal.

3. A user authentication system according to claim 2,  
wherein the information exchanged through the information  
10 communication channel is encrypted.

4. A user authentication system according to any of  
*Claim 1*  
~~claims 1 through 3,~~ wherein the two or more certification  
authorities dividedly record part of the biological individuality  
15 data obtained at the registration station but not recorded in the  
user authentication card, and one certification authority  
compares the biological individuality data of the user input at  
the authentication access terminal with the part of the  
biological individuality data stored in the certification  
20 authority in response to inquiry from the authentication access  
terminal or other certification authority for further  
authentication.

5. A user authentication system according to any of  
*Claim 1*  
25 ~~claims 1 through 4,~~ wherein the certification authority is  
provided with a memory device for recording the biological  
individuality data obtained at the registration station.

662021 09054460

2  
Claim 1  
6. A user authentication system according to any of  
~~claims 1 through 5~~, wherein plural kinds of biological  
individuality data are registered so that different transactions  
can be conducted in response to the kind of the input data.

5  
7. A user authentication device comprising an  
authentication-card reader for reading out information recorded  
in an authentication IC card, an identity acquisition device for  
inputting biological individuality data of a user, a judgment  
10 device for checking the biological individuality data of the  
authentication IC card read out by the authentication-card reader  
against the biological individuality data input on the spot  
through the identity acquisition device and for judging  
acceptance of the user, a communication unit for transmitting at  
15 least a part of the biological individuality data of the user  
input through the identity acquisition unit to a certification  
authority outside and receiving an authentication result of the  
certification authority, and a display device for displaying a  
judgment result.

20  
8. An authentication IC card comprising a CPU, an  
authentication file storing identity information, and an  
application file classified into files according to the depth of  
authentication, wherein when requested from the outside to  
25 present information recorded in the application file, the CPU  
compares identity information input from the outside with the  
identity information stored in the authentication file, and  
confirms the depth of authentication, whereby if an acceptance is

004450660 120229660

derived from the comparison, the information of the application file is presented through the CPU.

5 9. An authentication IC card comprising a CPU, an authentication file storing identity information, and an application file classified into files according to the depth of authentication, wherein when requested from the outside to present information recorded in the application file, the CPU outputs the identity information stored in the authentication  
10 file, whereby access to the application file is allowed through the CPU based on the judgment result from an external device.

10. An authentication IC card according to claim 8 or 9, wherein each file of the application file records an ID  
15 indicative of the authority to conduct each target transaction.

11. An authentication IC card according to any of claims 8 through 10, wherein qualification conditions to access each application file are pre-registered so that only the qualified  
20 persons are allowed to access the corresponding file.

12. An authentication IC card comprising a CPU, an authentication file storing identity information or both of identity information and authentication information, and an  
25 application file storing job programs or data classified according to the depth of authentication, and when access to the application file is requested from the outside, the authentication IC card allowing the access as a result of

662021"09054460

judgment based on the identity information or the authentication  
information of the authentication file, wherein the  
authentication file stores identity information on at least one  
second person other than the first person subject to personal  
5 authentication with the card, or authentication information on at  
least one organism with predetermining a job or data to request  
for authenticating the second person or organism, and when  
requested to execute such a specific job as to request for  
authenticating the second person or organism, or to show the data,  
10 the CPU compares identity information or authentication  
information input by the second person or the organism from the  
outside with the identity information or authentication  
information of the authentication file to allow execution of the  
specific job or showing the data when the authentication is  
15 acceptable.

13. An authentication IC card according to claim 12,  
wherein the CPU outputs the identity information or  
authentication information stored in the authentication file to  
20 the external device, whereby access to the application file is  
allowed through the CPU based on the judgment result from the  
external device.

14. An authentication IC card according to claim 12 or  
25 13, wherein authentication of the persons or organism is executed  
for both the first person and the second person or organism,  
whereby access to the application file is allowed when both has  
passed in the authentication.

00445060.120299

15. An authentication IC card according to any of claims 12 through 14, further comprising a file for electronic certificates on which the contents of authentication are recorded so as to present an electronic certificate indicative of the contents of the authentication used for access to the application file.

16. A lock control system comprising an IC card reader and an identity data input device, wherein the IC card reader reads out an IC card recording personal authentication data of a user so that identity data input through the identity data input device is checked with the personal authentication data recorded in the IC card, whereby a corresponding lock is opened when the user passes in the personal authentication.

17. A lock control system according to claim 16, wherein the personal authentication data recorded in the IC card include user's living body information data or information data created by the user.

18. A lock control system according to claim 16 or 17, wherein the IC card can selectively record plural kinds of personal authentication data.

19. A lock control system according to claim 18, wherein the lock is provided in each control district of a storage that is divided into plural control districts so that the personal

09445060-120299

authentication data can be selected for each control district.

Add 7

A

09445060 12029  
062021" 09054460